**DEPARTMENT OF THE ARMY**
**HEADQUARTERS, 4th INFANTRY DIVISION**
**FORT HOOD, TEXAS 76544-5200**

AFYB-CG

22 March 2007

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: 4ID, G6 Information Assurance (IA) Policy # 13: Web Servers

1. References:

   a. AR-25-1, Army Knowledge Management and Information Technology, 15 July 2005.

   b. AR 25-2, Information Assurance, 14 November 2003.

   c. AR 380-67, Personnel Security Program, 9 September 1988.

   d. DoD Directive 8500.1, "Information Assurance (IA)", 24 October 2002.

   e. DOD Instruction 8500.2, “Information Assurance (IA) Implementation”, 6 February 2003.

   f. DoD Instruction 5200.40, DoD Information Technology Security Certification and Accreditation (C&A) Process, 30 December 1997.

   g. DoD CIO Guidance and Policy Memorandum (G& PM) No. 8-8001 - "Global Information Grid (GIG)," 31 March 2000.

   h. DoD CIO Guidance and Policy Memorandum No 6-8510, "Department of Defense GIG Information Assurance and Information Assurance Implementation Guide", 16 June 2000.

2. Purpose of Policy:

   a. The U.S. Army Directorate of Information Management (DOIM) supports automated information systems (AIS) and communications systems requirements of numerous Military Commands, Garrison, and Tenant Organizations. With the growth and acceptance of the World Wide Web (Internet) as a primary communications resource, 4ID customer organizations are using customized “Web services” to promote their mission and capabilities to the general public.

   b. Given the “public” nature of Web connectivity, 4ID supported web services are vulnerable to inherent IA risks. There are two distinct sets of vulnerabilities: Web services exposed to the general public via Internet, NIPRNET, or DREN access; and internal web services intended solely for internal use with access by users that does not transit the Internet, NIPRNET, or DREN. This policy provides a consistent framework for 4ID IT/IA organizations to minimize and manage web services IA vulnerabilities under both scenarios.

3. Applicability: This policy applies to all soldiers, civilians, and contractors who plan, deploy, configure, operate, and maintain data communications resources directly or indirectly attached to 4ID networks.

4. Responsibilities.

   a. Organization Directors and Web Services Owners:

It is the 4ID policy that web services owners are responsible for ensuring that required networking and Information Assurance (IA) solutions are implemented to safeguard information content and integrity of web services for which they are responsible.[1]

b. Directors of 4ID AIS/IA service providers:

It is the 4ID policy that Directors of 4ID IT/IA service providers are responsible for providing IT / IA solutions that protect the web services they operate and to protect the 4ID infrastructure from compromise through hosted web site4s.

c. 4ID Information Assurance Manager (IAM):

(1) The 4ID IAM will centrally oversee and verify compliance with 4ID AIS / IA policies and solutions.

(2) The IAM will provide a central location for archiving, evaluating, and validating 4ID IA documentation, configuration management records, and usage logs applicable to web services operation and security.

d. All 4ID personnel and tenants will report suspected unauthorized activity on 4ID web sites to their respective Information Assurance Manager (IAM), Information Assurance Network Manager/Officer (IANM/O), or Information Assurance Security Officer (IASO). Depending upon the nature of the unauthorized activity the Computer Incident Response Team may be activated to document and resolve an incident.

5. Policies on Web Server Security:

a. Public and Internal Web services

(1) Web Server Installation Controls: Root or Administrator access to Web Server files will be restricted to the server console. Root equivalence or Domain Administrator accounts may be assigned to administrators through a strong user ID and password assignment and then allowed remote access. The goal is accountability with user ID granularity for changes and updates made to the Web Server.

(2) File access restrictions will be explicitly configured according to the requirements of the web functionality, but will not be the default configuration, which could grant liberal access privileges to other users on the system.

(3) Web server startup configuration: Web servers will be started on nonstandard ports to reduce the risk of damage in case a server is compromised.

(4) File Access Permission Controls: File access permissions will specify who can read, write, or execute a file on the web server. Files read by the web server will be placed in a server root or document root directory that has been renamed from the default configuration to a specific location known to the web application, and unknown by or hidden from the general user community. The files of importance in the server root are the configuration files, log files, CGI program sources, CGI program executables, and administrative files and programs. The server root files will be neither visible nor accessible to anyone inside or outside the organization, except the web system administrators who install and configure the server.

(5) User's outside the web server's admin group will not have read or write permissions to any files in the server root. The access control permissions for files in the server root, while barring other users, will allow the web server to read its files.

(6) Escalating Client Privilege Controls: Each subordinate or child process initiated through a web request does not necessarily have to run at the super user level. Unless otherwise required, configure the Web server either to switch its executing privilege to a non-privileged user or configure the child process to execute as a non-privileged user. With this configuration, if exploitation does occur, the damage can be contained or restricted to the minimum privilege level.

(7) Automatic Directory Listing: If possible, automatic directory listings will be turned off, or alternatively every directory in the root will have an index.html file.

(8) Server Side Includes (SSIs): SSIs will be disabled in the server to prevent imbedded commands in an HTML document from executing on Web hosts with Web server privileges.

(9) Symbolic link following: Disable this option.

(10)To control access to sensitive documents from the Web server, depending on the level of authentication required, use client hostname and IP address restrictions, user and password authentication, or digital certificates. In using client hostname and IP address restrictions, use a Domain Name Service (DNS) to verify the hostname and IP address accompanying the access request. Also, if appropriate, use router Access Control Lists to restrict access to the Web server.

(11)User and Password Authentication: This technique compares the user ID and password with an established database of acceptable users and their passwords. In this case, the password file will be renamed from the default and hidden.

(12)Digital Certificates or SSL: Invoke this technique to protect information flowing to and from the Web site and to provide higher levels of user authentication.

(13)Each Web server will inevitably have different user requirements and a security policy will be developed for each Web host and applied to allow the specific functionality required consistent with prudent security controls.

(14)CGI scripts pose serious potential risks to Web servers, including the ability for remote Web clients to execute system commands that may:

(a) Read, replace, modify, or remove files,
(b) Mail files back over the Internet,
(c) Execute programs downloaded on the server such as a password sniffer or a network daemon that will provide unauthorized telnet access to the server, or
(d) To launch a denial-of-service attack by overloading the server CPU with a computation-intensive tasks such as exhaustive file system searches.

(15)CGI Scripts: CGI scripts will be analyzed for programming errors and corrected prior to being put into the production environment.

(16)Remove all CGI scripts not required for Web server functionality (includes utility scripts).

(17)CGI Programs: Configure the directories from which CGI programs can execute. Some programs use default directory structures and execute any program ending with .cgi or.pl from anywhere under the server root. CGI scripts will be analyzed for security issues prior to being placed into production. Restrict the directories from which CGI scripts can execute. A single directory under the server root will be established from which only approved CGI scripts can execute. The server will be configured so that when any script or program in this directory is requested in a Web request, the program will execute rather than have the source downloaded.

(18)Protect Source Code: The software source code stored in cgi-src will be protected from unauthorized access. Backup files for CGI scripts and sources will be removed from the cgi-bin and cgi-src directories.

(19)Once a set of stable CGI programs has been established for the cgi-bin and source directories, a digital hash, such as MD5, will be made of the directories. This serves as a version control mark and can provide an indication of file tampering or carelessness.

(20)Do not place shell interpreters in the cgi-bin directory.

(21)Database controls such as access control mechanisms (user ID and passwords, plus assignment of user rights - read, write, delete, modify, etc.) and data encryption will be utilized when protection of data from unauthorized disclosure and database integrity are important.

(22)Wipe temporary database files from the server as soon as the file has served its purpose.

(23)Once the Web site is properly configured, it will be cached with the original of the server files stored in a server location that refreshes the cache on a recurring and frequent basis. The location of the original files (e.g., CD-ROM drive on the Web Server) will not allow writes to the drive. Changes will be made to the Web site by producing an updated set of files and loading them to the CD-ROM drive and refreshing the site from the CD.

b. Public Web services:

(1) All Army publicly accessible web sites residing on 4ID installations will be registered with the 4ID IANM and will be hosted on the Army Regional Web Cache.

(2) Incoming TCP port 80 and TCP port 8080 traffic will be blocked at all border router connections to WANs (NIPRNET, DREN, etc). Exceptions may be made for traffic addressed to non-Army organizations such as DLA and DTIC that demonstrate to the 4ID IANM that they have adequate safeguards in place.

(3) Web servers will be located in a security zone protected by a firewall that contains only web servers. Public web servers will communicate with the cache on non-standard ports. TCP port 80 or 8080 will not be used.

(4) The firewall will permit traffic to/from the cache IP address, the IP addresses of the web server administrators/content managers, and domain controllers (if required) only. Traffic to/from all other IP addresses will be blocked.

(5) The firewall will permit traffic between the web server and the cache only on the non-standard port selected for web server/cache communications. The firewall will permit traffic initiated from the administrators/content managers to the web server and will prohibit traffic initiated from the web server to the administrators/content managers. Only the ports actually required will be opened between the web server and the administrators/content managers and domain controllers.

(6) If there is more than one web server in the web server security zone, a private VLAN (CISCO switches) or equivalent will be used to ensure that they cannot communicate with each other without first passing through the firewall.

c. Internal Web Sites:

(1) All 4ID internal Web sites will be protected by a router or switch that provides exclusive routing to specific internal Web sites and verifies that the point of origin of the person accessing the site is from an internal IP address

(2) All 4ID internal Web sites will be protected by a firewall through which access control filters will be configured to restrict Web access to internal IP points of origin. Upon receiving a web inquiry through a router, the access path will be defined and routed to the Web site. The firewall will block all traffic originated by the web server except that addressed to domain controllers, if required. Only those ports actually required for the domain controller communications will be opened.

(3) TCP ports 80 and 8080 will be blocked by the firewall. Internal Web sites will have certificates installed and operate HTTPS only.

(4) If there is more than one web server in the web server security zone, a private VLAN (CISCO switches) or equivalent will be used to ensure that they cannot communicate with each other without first passing through the firewall.

6. Non-Compliance:

a. All unauthorized access attempts or unauthorized activity on the web site will be logged and provided to the IANM for review and follow-up action as deemed appropriate. Attempts to disable a public web site, or initiate a denial of service attack will, or alter web pages, will prompt an alert to the Computer Incident Response Team for immediate action.

b. Web site configurations will be audited annually for compliance with this policy. Web site administrators will be held accountable for the web site configuration. If a web site is found to be out of compliance with this policy the web site administrator will be held accountable.

7. POC for this policy is the 4ID Information Assurance at DSN 737-0785 or commercial 254-287-0785.

JEFFERY W. HAMMOND
MG, USA
Commanding